Jon Postel

Network Working Group
Request for Comments: 1038

M. St. Johns
IETF
January 1988

Draft Revised IP Security Option

Status of this Memo

This RFC is a pre-publication draft of the revised Internet Protocol Security Option. This draft reflects the version as approved by the Protocol Standards Steering Group. It is provided for informational purposes only. The final version of this document will be available from Navy Publications and should not differ from this document in any major fashion.

This document will be published as a change to the MIL-STD 1777, "Internet Protocol". Distribution of this memo is unlimited.

9.3.13.1 Internet Options Defined.

The following internet options are defined:

CLASS	NUMBER	LENGTH	DESCRIPTION
0	00000	-	End of Option list: This option occupies only 1 octet; it has no length octet.
0	00001	-	No Operation: This option occupies only 1 octet; it has no length octet.
0	00010	var.	Basic Security: Used to carry security level and accrediting authority flags.
0	00011	var.	Loose Source Routing: Used to route the datagram based on information supplied by the source.
0	00101	var.	Extended Security: Used to carry additional security information as required by registered authorities.
0	01001	var.	Strict Source Routing: Used to route the datagram based on information supplied by the source.
0	00111	var.	Record Route: Used to trace the route a datagram takes.
0	01000	4	Stream ID: Used to carry the stream identifier.
2	00100	var.	Internet Timestamp: Used to accumulate timing information in transit.

9.3.15.3 DoD Basic Security.

Option type: 130 Option length: variable; minimum length: 4

The option identifies the U.S. security level to which the datagram is to be protected, and the accrediting authorities whose protection rules apply to each datagram.

The option is used by accredited trusted components of an internet to:

a. Validate the datagram as appropriate for transmission from the source.

b. Guarantee that the route taken by the datagram (including the destination) is protected to the level required by all indicated accrediting authorities.

c. Supply common label information required by computer security models.

This option must be copied on fragmentation. This option appears at most once in a datagram.

The format of this option is as follows:

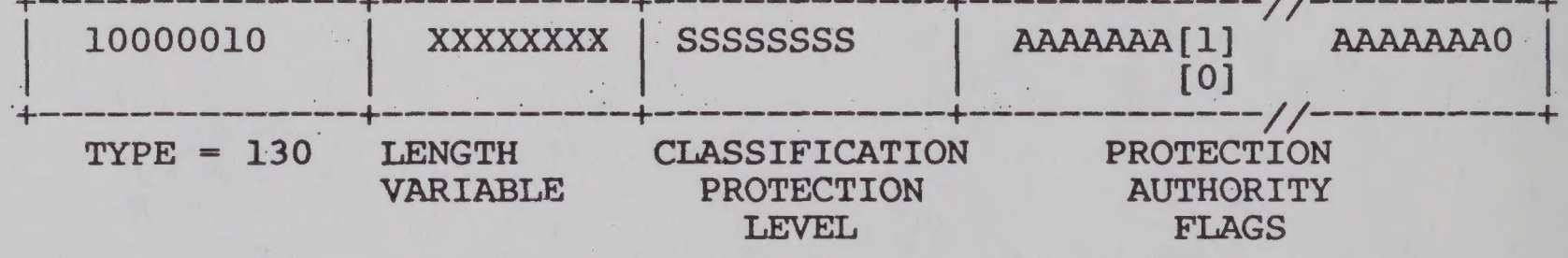

FIGURE 10-A. SECURITY OPTION FORMAT

9.3.15.3.1 Length.

The length of the option is variable. The minimum length option is 4.

9.3.15.3.2 Classification Protection Level.

This field specifies the U.S. classification level to which the datagram should be protected. The information in the datagram should be assumed to be at this level until and unless it is regraded in accordance with the procedures of all indicated protecting

authorities. This field specifies one of the four U.S. classification levels, and is encoded as follows:

11011110	-	Top Secret
10101101	-	Secret
01111010	-	Confidential
01010101	-	Unclassified

9.3.15.3.3 Protection Authorities Flags.

This field indicates the National Access Program(s) with accrediting authority whose rules apply to the protection of the datagram.

a. Field Length: This field is variable in length. The low-order bit (Bit 7) of each octet is encoded as "zero" if it is the final octet in the field, or as "one" if there are additional octets. Currently, only one octet is needed for this field (because there are less than seven authorities), and the final bit of the first octet is coded as "zero".

b. Source Flags: The first seven bits (Bits 0 through 6) in each octet are source flags which are each associated with an authority as indicated below. The bit corresponding to an authority is "one" if the datagram is to be protected in accordance with the rules of that authority.

9.3.15.3.4 Usage Rules.

Use of the option requires that a host be aware of 1) the classification level, or levels, at which it is permitted to operate, and 2) the protection authorities responsible for its certification. The achievement of this is implementation dependent. Rules for use of the option for different types of hosts are given below.

9.3.15.3.4.1 Unclassified Hosts, including gateways.

a. Output: Unclassified hosts may either use or not use the option. If it is used, classification level must be unclassified, bit 0 of the accreditation field (GENSER) must be one, and all other bits of the accreditation field must be 0. While use of the option is permitted, it is recommended that unclassified hosts interested in maximizing interoperability with existing non-compliant implementations not use the option.

b. Input: Unclassified hosts should accept for further processing IP datagrams without the option. If the option is present on an incoming IP datagram, then the datagram is accepted for further processing only if the classification level is

unclassified, bit 0 of the accreditation field (GENSER) is one, and all other bits of the accreditation field are zero. Otherwise, the out-of-range procedure is followed.

9.3.15.3.4.2 Hosts accredited in the Dedicated, System-High, or Compartmented Modes at a classification level higher than unclassified.

a. Output. The use of the option is mandatory. The classification level should be the dedicated level for dedicated hosts and the system-high level for system-high and compartmented hosts. The accrediting authority flags should be one for all authorities which have accredited the hosts, and zero for all other authorities.

b. Input. If 1) the option is present, 2) the classification level matches the host classification level, and 3) the accrediting authority flags for all accrediting authorities of the receiving host are one, and all others are zero, the IP datagram should be accepted for further processing. Otherwise, the out-of-range procedure is followed.

9.3.15.3.4.3 Hosts accredited in the Multi-Level or Controlled Mode for network transmission.

a. Output. The use of the option is mandatory. The classification level of an IP datagram should be within the range of levels for which the host is accredited. The protection authorities flags should be one for all authorities under whose rules the datagram should be protected.

b. Input. In the specific case where a multi-level or controlled host is accredited to directly interface with an unclassified environment, the host may accept IP datagrams without a basic security option. Such datagrams should be assumed to be implicitly labelled unclassified, GENSER, and should be so labelled explicitly if they are later output. In all other cases, the IP datagrams should have the basic security option on input, and the out-of-range procedure should be followed if it is not.

There are two cases to be considered where the option is present. The first case is where the system environment permits the values in the option to be trusted to be correct for some range of values; the second is where the values cannot be trusted to be correct. For each multi-level or controlled host, every input channel for IP datagrams must be considered and classed appropriately. If a channel does have a trusted range, then the values of both the classification level and the protection authorities are checked to insure that they fall within that range and the range of accredited values for the

receiving host. If within both ranges, the IP datagram is accepted for further processing; otherwise the out-of-range procedure is followed. If the label cannot be trusted, then the receiving host must possess some accredited means of knowing what the correct marking should be (e.g., a trusted channel to a system-high host at a known level). On receipt of an IP datagram, the host compares the actual values in the option to the correct values. If the values match, the datagram is accepted for further processing; otherwise, the out-of-range procedure is followed.

9.3.15.3.4.4 Out-Of-Range Procedure.

If an IP datagram is received which does not meet the input requirements, then:

a) The data field should be overwritten with ones.

b) If the problem is a missing required Basic or Extended security option, an ICMP "parameter problem" message is sent to the originating host with the code field set to 1 (one) to indicate "missing required option" and the pointer field set to the option type of the missing option. Otherwise, an ICMP "parameter problem" message is sent to the originating host with code field set to 0 (zero) and with the pointer field pointing to the position of the out-of-range security option.

c) If the receiving host has an interface to a local security officer or equivalent, the problem should be identified across that interface in an appropriate way.

9.3.15.3.4.5 Trusted Intermediary Procedure.

Certain devices in the internet may act as intermediaries to validate that communications between two hosts are authorized, based on a combination of knowledge of the hosts and the values in the IP security option. These devices may receive IP datagrams which are in range for the intermediate device, but are either not within the acceptable range for the sender, or for the ultimate receiver. In the former case, the datagram should be treated as described above for an out-of-range option. In the latter case, a "destination unreachable" ICMP message should be sent, with the code value of 10 (ten), indicating "Communication with Destination Host Administratively Prohibited".

9.3.15.4 DoD Extended Security Option

Option type: 133 Option length: variable

This option permits additional security related information, beyond that present in the Basic Security Option, to be supplied in an IP datagram to meet the needs of registered authorities. If this option is required by an authority for a specific system, it must be specified explicitly in any Request for Proposal. It is not otherwise required. This option must be copied on fragmentation. This option may appear multiple times within a datagram.

The format for this option is as follows:

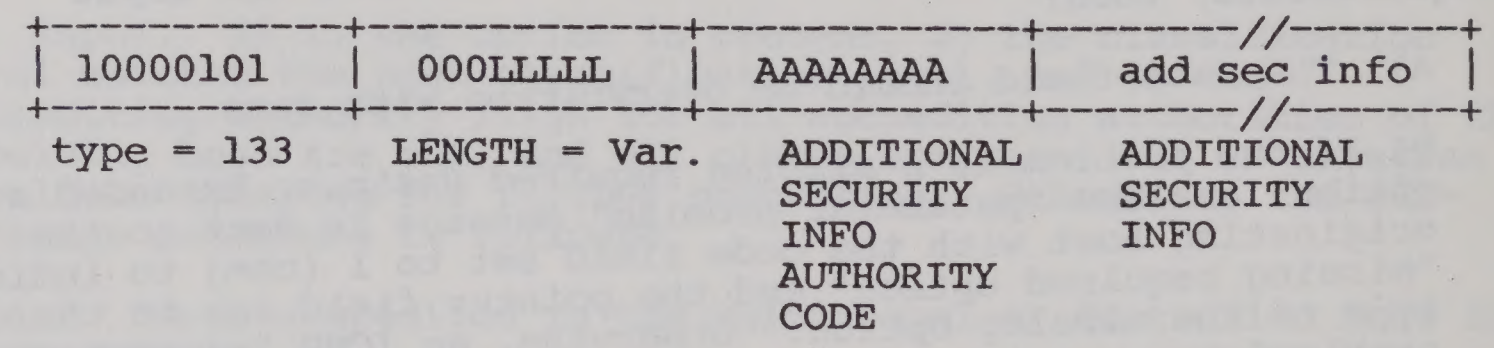

FIGURE 10-B.

9.3.15.4.1 Additional Security Info Authority Code.

length = 8 bits

The values of this field are assigned by DCA Code R130, Washington, D.C. 20305-2000. Each value corresponds to a requestor who, once assigned, becomes the authority for the remainder of the option definition for that value.

9.3.15.4.2 Additional Security Information.

length - variable

This field contains any additional security information as specified by the authority.

BIT NUMBER	AUTHORITY
0	GENSER
1	SIOP
2	DSCCS-SPINTCOM
3	DSCCS-CRITICOM
4-7	Unassigned

AUTHORITY	SOURCE OF ANNEX DESCRIBING CURRENT CODING OF ADDITIONAL SECURITY INFORMATION
GENSER National Access Program, less SIOP	Defense Communications Agency ATTN: Code R130 Washington, DC 20305
SIOP National Access Program	Department of Defense Organization of the Joint Chiefs of Staff Attn: J6T Washington, DC
DSCCS-SPINTCOM National Access Program	Defense Intelligence Agency Attn: DSE4 Bolling AFB, MD
DSCCS-CRITICOM National Access Program	National Security Agency 9800 Savage Road Attn: T03 Ft. Meade, MD 20755-6000